Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ciencias Matemáticas
Escuela Profesional de Investigación Operativa

Asignación de frecuencias de campañas de concientización para prevenir incidentes de seguridad de la información usando análisis jerárquico de procesos en Financiera Oh

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Licenciado en Investigación Operativa

AUTOR

Jesús Oliverio BALTAZAR MELGAREJO

ASESOR

Dr. Carlos ORTEGA MUÑOZ

Lima, Perú

2022



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

https://creativecommons.org/licenses/by-nc-sa/4.0/

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Baltazar, J. (2022). *Asignación de frecuencias de campañas de concientización para prevenir incidentes de seguridad de la información usando análisis jerárquico de procesos en Financiera Oh*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ciencias Matemáticas, Escuela Profesional de Investigación Operativa]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Jesús Oliverio Baltazar Melgarejo
Tipo de documento de identidad	DNI
Número de documento de identidad	45475285
URL de ORCID	-
Datos de asesor	
Nombres y apellidos	Carlos Ortega Muñoz
Tipo de documento de identidad	DNI
Número de documento de identidad	10196265
URL de ORCID	https://orcid.org/0000-0001-8663-4095
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Esther Berger Vidal
Tipo de documento	DNI
Número de documento de identidad	08766040
Miembro del jurado 1	
Nombres y apellidos	José Carlos Oré Luján
Tipo de documento	DNI
Número de documento de identidad	06119405
Datos de investigación	
Línea de investigación	A.3.3.3. Toma de decisiones

Grupo de investigación	No aplica.
Agencia de financiamiento	Sin financiamiento.
Ubicación geográfica de la investigación	Universidad Nacional Mayor de San Marcos País: Perú Departamento: Lima Provincia: Lima Distrito: Lima Coordenadas geográficas Latitud: -12.058333 Longitud: -77.083333
Año o rango de años en que se realizó la investigación	Julio 2022
URL de disciplinas OCDE	Matemáticas aplicadas https://purl.org/pe-repo/ocde/ford#1.01.02

Anexo 6

ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL EN LA MODALIDAD VIRTUAL PARA OBTENCIÓN DEL TÍTULO PROFESIONAL DE LICENCIADO(A) EN INVESTIGACIÓN OPERATIVA

(PROGRAMA DE TITULACIÓN PROFESIONAL 2022-I)

En la Ciudad Universitaria, Facultad de Ciencias Matemáticas, siendo las 14:00 horas del día sábado 23 de julio del año 2022, se reunieron los docentes designados como Miembros del Jurado Evaluador del Trabajo de Suficiencia Profesional:

Dra. Esther Berger Vidal	(Presidente)
Mg. José Carlos Oré Luján	(Miembro)
Dr. Carlos Ortega Muñoz	(Miembro-Asesor)

Para la sustentación del Trabajo de Suficiencia Profesional intitulada: ASIGNACIÓN DE FRECUENCIAS DE CAMPAÑAS DE CONCIENTIZACIÓN PARA PREVENIR INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN USANDO ANÁLISIS JERÁRQUICO DE PROCESOS EN FINANCIERA OH, presentada por el señor Bachiller Baltazar Melgarejo, Jesús Oliverio, para obtener el Título Profesional de Licenciado en Investigación Operativa.

Luego de la exposición del Trabajo de Suficiencia Profesional, la Presidenta invitó al expositor a dar respuesta a las preguntas formuladas.

Realizada la evaluación correspondiente por los miembros del jurado, el expositor mereció la aprobación ***Bueno*** con un calificativo promedio de: **Dieciséis (16).**

A continuación, los miembros del jurado dan manifiesto que el participante señor Bachiller Baltazar Melgarejo, Jesús Oliverio, en virtud de haber aprobado la sustentación de su Trabajo de Suficiencia Profesional, será propuesto para que se le otorgue el Título Profesional de Licenciado en Investigación Operativa.

Siendo las 14:45 horas, se levantó la Sesión, firmando para constancia la presente Acta en tres (3) copias originales o archivo PDF.

PRESIDENTA
Dra. Esther Berger Vidal

MIEMBRO
Mg. José Carlos Oré Luján

MIEMBRO-ASESOR
Dr. Carlos Ortega Muñoz

Firmado digitalmente por
VELASQUEZ PINO Carmela Catalina
FAU 20148092282 soft
Motivo: Soy el autor del documento
Fecha: 30.11.2022 23:15:58 -05:00

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. Decana de América
FACULTAD DE CIENCIAS MATEMÁTICAS
ESCUELA PROFESIONAL DE INVESTIGACIÓN OPERATIVA

INFORME DE EVALUACIÓN DE ORIGINALIDAD

La Directora de la Escuela Profesional de Investigación Operativa, Mg. Carmela Catalina Velásquez Pino, informa lo siguiente:

1. Operador del programa informático de similitudes: Dr. Paulo Cesar Olivares Taipe
2. Documento evaluado:
   Asignación de frecuencias de campañas de concientización para prevenir incidentes de Seguridad de la Información usando Análisis Jerárquico de Procesos en Financiera Oh
3. Autor de la tesis: Jesús Oliverio BALTAZAR MELGAREJO
4. Fecha de recepción de la tesis: 27/11
5. Fecha de aplicación del programa informático de similitudes: 29/11
   - Software utilizado: Turnitin
6. Configuración del programa detector de similitudes:
   - Excluye textos entrecomillados
   - Excluye bibliografía
   - Excluye cadenas menores a 40 palabras
7. Porcentaje de similitudes según programa detector de similitudes:
8. Fuentes originales de las similitudes encontradas: 6%
   Fuentes de internet: 7%
   Publicaciones: 2%
9. Calificación de originalidad:
   - El documento mencionado cumple criterios de originalidad, sin observaciones

Lima, 29 de noviembre 2022

Mg. Carmela Catalina Velásquez Pino
Directora

Agradezco a Dios de quien todo procede,
a mi esposa e hijas por la paciencia en este periodo,
a mis padres por el impulso y ánimo
para terminar este camino
y al profesor Juan J. Toledo R.,
con quien inicié este trabajo.

Dedico este esfuerzo y resultados
a mi esposa y a mis hijos.

Resumen

Asignación de frecuencias de campañas de concientización para prevenir incidentes de Seguridad de la Información usando Análisis Jerárquico de Procesos en Financiera Oh

Baltazar Melgarejo Jesús Oliverio

Julio 2022

Título obtenido : Licenciado en Investigación Operativa

El Sars-Cov2 trajo consigo cambios en el estilo de vida del mundo entero, obligándonos a realizar muchas de nuestras actividades habituales desde el hogar. Esto trajo consigo que aquellas personas que se desenvolvían en una oficina, aula o fábrica y que tuvieran la capacidad de desarrollar sus funciones desde casa, puedan seguir operando de forma remota. Sin embargo, los trabajadores se vieron expuestos a riesgos que antes eran mitigados por todas las herramientas de seguridad digital dentro de su centro de labores: correos falsos, archivos maliciosos, mensajes de suplantadores, llamadas sospechosas, ingeniería social, entre otros.

Ante este incremento de ciberdelincuencia, no solo en el Perú, sino en el mundo entero como lo detalla la empresa de seguridad Fortinet, Financiera Oh requiere determinar qué temas deben reforzarse a los trabajadores, de modo que cuenten con la capacidad suficiente de proteger la información importante de la empresa que manejan desde su nueva sede de labores.

En este sentido, el área de Seguridad de la Información desarrolla un plan de concientización utilizando el análisis jerárquico de procesos para determinar la frecuencia de campañas que la empresa debe enviar a sus colaboradores para prevenir un incidente de seguridad.

PALABRAS CLAVE: Teoría de decisiones, matriz de preferencias, criterios múltiples, análisis jerárquico de preferencias (AHP).

Abstract

Frequency assignment of awareness campaigns to prevent Information Security incidents using Analytic Hierarchy Process in Financiera Oh

Baltazar Melgarejo Jesús Oliverio

July 2022

Graduate : Operations Research

Sars-Cov2 brought changes in the lifestyle of the entire world, forcing us to carry out many of our usual activities from home. From this it follows that the person's activities are carried out in an office, classroom or factory and that they have the ability to carry out their functions from home, they can continue to operate remotely. However, workers were exposed to risks that were previously mitigated by all the digital security tools within their workplace: fake emails, malicious files, messages from impersonators, suspicious calls, social engineering, among others.

Faced with this increase in cybercrime, not only in Peru, but throughout the world, as detailed by the security company Fortinet, Financiera Oh needs to determine what should be reinforced for workers, so that they have sufficient capacity to protect important information. of the company they run from their new headquarters.

In this sense, the Information Security area develops an awareness plan using the hierarchical analysis of processes to determine the frequency of campaigns that the company must send to its employees to prevent a security incident.

KEYWORDS: Decision theory, matrix of preferences, multiple criteria, analysis hierarchical preference (AHP).

ÍNDICE

I. INTRODUCCIÓN 1
II. INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD 3
1. Descripción de la organización 3
2. Gerencia de Seguridad de la Información y prevención de fraudes 3
3. Periodo de duración de la actividad 1
III. DESCRIPCIÓN DE LA ACTIVIDAD 2
1. Objetivo de la actividad 3
2. Problemática 3
3. Metodología 4
3.1. Reconocimiento del problema y estructuración 6
3.1.1. Determinación del equipo de trabajo 6
3.1.2. Identificación del problema 7
3.1.3. Definición del objetivo 7
3.2. Estimaciones y evaluación 8
3.2.1. Elección de criterios, subcriterios y alternativas 8
Criterios 8
Subcriterios 9
Alternativas 10
3.2.2. Árbol de jerarquías 13
3.2.3. Matriz de ponderaciones 13
Evaluación de criterios y subcriterios 13
Evaluación de alternativas 15
Proceso de síntesis 16
Prueba de Consistencia 16
3.3. Análisis de sensibilidad 17
3.3.1. Análisis de solidez del modelo 17
3.3.2. Prioridades globales 17
3.4. Resultados 18
3.4.1. Reconocimiento del problema y estructuración 18
Definición de objetivo 18
Identificación de criterios, subcriterios y alternativas 18
Árbol de jerarquías 20
3.4.2. Estimaciones y evaluación 22

Análisis de sensibilidad 25
IV. CONCLUSIONES 28
V. RECOMENDACIONES 29
REFERENCIAS 30

I. INTRODUCCIÓN

La Seguridad de la Información ha logrado posicionarse en los últimos años como uno de los pilares más importantes en las organizaciones a nivel mundial, sin embargo, lejos de ser una adecuación voluntaria, ha sido un cambio forzoso ante el gran incremento de ciberataques en los cinco continentes. Estas situaciones, intensificadas por el confinamiento a causa del COVID-19, han causado grandes pérdidas a las organizaciones y no solo económicas, sino también reputacionales y compromisos regulatorios. Para tener una idea más clara, solo el año 2020, según la empresa tecnológica Fortinet, los intentos de ciberataques en Perú ascendieron a 2.6 billones, mientras que a nivel Latinoamérica hubo 41 billones de intentos de infiltrarse en organizaciones y/o redes privadas, superando superlativamente los registros y estadísticas de años anteriores.

Podríamos objetar que la estadística de la empresa tecnológica en mención refiere a intentos mas no a materialización de ciberataques, sin embargo, las empresas que se han visto afectadas por filtración de datos o ataques de *ransomware*, en mucho de los casos, informaron a los entes reguladores que el vector de ataque de estos incidentes involucraban a colaboradores que eran engañados mediante correos, llamadas, páginas falsas o dispositivos a su alcance. Ante esto ¿qué se puede hacer si el eslabón más débil son las personas?

Por ello, Financiera Oh, encargó al área de Seguridad de la Información y Ciberseguridad evaluar la efectividad del plan concientización a los colaboradores en materia de incidentes de seguridad y estructurarlo de manera que pueda responder a los constantes cambios y novedades que a nivel mundial se van presentando en el rubro financiero, con miras a brindar a los colaboradores herramientas prácticas para evitar que sean engañados y utilizados para materializar ciberataques. Ante este encargo, se decidió aplicar una herramienta de Investigación de Operaciones que permita sustentar el cronograma de concientización para prevenir incidentes de seguridad de la información en base a la experiencia de los especialistas de la materia en la organización y respondiendo a la realidad de la empresa, entorno, nacional y mundial en temas de ciberseguridad.

El informe está dividido en cuatro grandes secciones las cuales van permitiendo al lector entender la realidad de la organización, para luego descender al detalle de las actividades. Es por ello que en la primera parte se encontrará información del lugar donde se aplicó el AHP, la estructura organizativa y las áreas involucradas.

En la segunda sección se podrá conocer la metodología y las actividades planificadas, detallándose el objetivo, la problemática y cada una de las tareas realizadas para abordar el problema con la herramienta de Investigación Operativa en mención, así como los resultados registrados del Análisis Jerárquico de Procesos, la perspectiva de cada evaluador y los resultados alcanzados para tomar las decisiones.

Como tercera sección se detallan las conclusiones a las que se llegan luego del ejercicio aplicado y finalmente en la última sección las recomendaciones presentadas a la alta gerencia, producto del análisis realizado

II. INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD

1. Descripción de la organización

Financiera Oh! S.A. es una empresa del sector financiero domiciliada en Av. Aviación 2405, San Borja; regulada por la Superintendencia de Banca, Seguros y AFP (SBS), así como por el Ministerio de Justicia, a través de la Autoridad Nacional de Protección de Datos Personales (ANPD). Esta organización ofrece tarjetas de crédito, seguros y crédito efectivo, además de productos pasivos, como compensación por tiempo de servicio (CTS) y depósito a plazo fijo (DPF).

La entidad cuenta con un área especializada en Seguridad de la Información y Ciberseguridad la cual, como parte de sus funciones, en el marco de las regulaciones vigentes SBS G-140:2009, SBS-504:2021 y Ley N° 29733; y ante el aumento a nivel mundial de eventos que comprometen la seguridad de la información a raíz del confinamiento por el Sars-Cov2, desarrolló una estrategia de concientización para prevenir incidentes de seguridad y ciberseguridad utilizando el análisis jerárquico de procesos.

La organización tiene como propósito “ayudar a los peruanos a disfrutar el presente mientras construimos juntos su futuro” (Financiera Oh, 2021)

2. Gerencia de Seguridad de la Información y prevención de fraudes

La Gerencia de Seguridad de la Información pertenece a la División de Administración y Operaciones en Financiera Oh! S.A. Está conformado por un grupo de profesionales de Investigación Operativa, Ingeniería Industrial e Ingeniería de Sistemas, los cuales velan por preservar la confidencialidad, integridad y disponibilidad de la información importante de la entidad. Sus funciones son las siguientes:

- Implementar un modelo de gobierno y gestión de Seguridad de la Información y Ciberseguridad cuyo propósito principal es proteger los activos de información de clientes y de la empresa
- Desarrollar un programa de concientización en Seguridad de la Información y Ciberseguridad para modelar el comportamiento individual y organizacional de sus grupos de interés para proteger la información.
- Asegurar la vigencia, razonabilidad y efectividad de la política, las normas, los procedimientos y las guías asociadas para su aplicación en las áreas, los procesos y roles de la empresa, así como la participación de todos los grupos de interés vinculados.

La estructura de la organización es la siguiente:

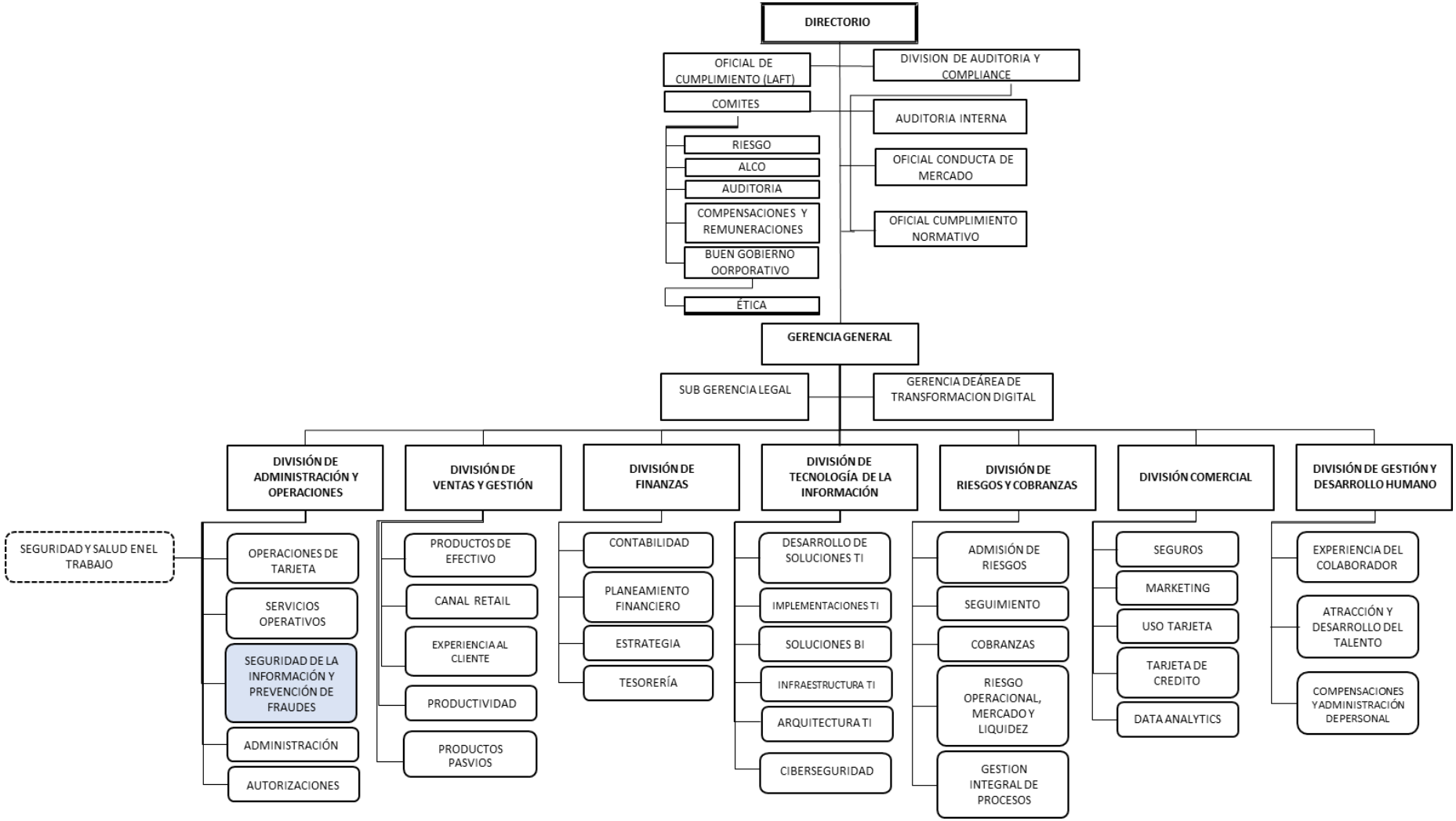

GRÁFICO N°1: Organigrama organizacional
(Financiera Oh, 2021)

3. Periodo de duración de la actividad

Esta actividad involucró como público objetivo a todos los colaboradores de la entidad y como equipo ejecutor al área de Seguridad de la Información. El estudio y evaluación, de forma excepcional para este caso, se realizaron entre los meses de enero y febrero del 2021, debido a la disponibilidad del equipo y por los recursos a consumir para la aplicación de la nueva metodología; y el despliegue de las campañas se realizaron durante todo el año a partir del mes de marzo, las cuales consistieron en piezas gráficas diseñadas con los temas de elegidos en el análisis y enviadas mediante correo electrónico a cada uno de los miembros de la empresa. Esta actividad era parte del cronograma de trabajo anual de la gerencia, la cual se sustentó utilizando la herramienta de Investigación Operativa.

III. DESCRIPCIÓN DE LA ACTIVIDAD

Las disposiciones regulatorias con respecto a Seguridad de la Información exigen a las entidades financieras que, como parte del compromiso de la alta gerencia, el área encargada de velar por la confidencialidad, integridad y disponibilidad de la información, presente un plan de trabajo anual al Directorio que incluya las actividades a realizar, los proyectos y metas en relación con esta disciplina. La metodología que se emplea para la estructuración del plan de trabajo se basa en la norma ISO/IEC 27001[*], la cual establece el PDCA[†] como referente para la implementación del Sistema de Gestión de Seguridad de la Información.

Esta actividad de planeamiento es ejecutada por el Supervisor de Seguridad de la Información durante los meses de noviembre y diciembre del año anterior, en coordinación con su equipo a cargo. En este ejercicio se evalúan los resultados del año y se consideran las actividades correspondientes para el periodo a empezar. El contenido mínimo que debe considerarse está estipulado por la G-140:2009 y su actualización en curso SBS-540:2021, las cuales establecen los dominios y objetivos de control a implementar para asegurar la información de la entidad.

Como parte de estos requerimientos, el nuevo reglamento establece el deber de la empresa de mantener planes operativos que involucren la capacitación y difusión en materia de seguridad de la información y ciberseguridad para asegurar la efectividad del sistema de Gestión de Seguridad de la Información y Ciberseguridad[‡] (SGSI), es decir, que existe una obligación regulatoria de concientizar a los colaboradores de tal manera que sean capaces de mantener el SGSI y, por supuesto, proteger toda la información importante de la empresa.

Asumiendo esta directriz, la actividad tuvo como finalidad determinar la cantidad de cada tema a tratar en las campañas de concientización que permitieran prever incidentes de seguridad.

---

[*] International Organization for Standardization (2013). *ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT*. https://www.iso.org/isoiec-27001-information-security.html

[†] PDCA – Plan, Do, Check, Act. Es la metodología utilizada en las normas ISO, la cual consiste en las fases de planificar, hacer, validar y actuar.

[‡] Superintendencia de Banca, Seguros y AFP (febrero de 2021). *Reglamento de Seguridad de la Información y Ciberseguridad.* Art. 13. Actividades planificadas.

1. Objetivo de la actividad

Aplicar una metodología que permita a Financiera Oh, en base a criterios específicos e información disponible, priorizar los temas de concientización a colaboradores para prevenir incidentes de Seguridad en la empresa, con el fin de asignar el número apropiado de campañas de acuerdo con múltiples criterios.

2. Problemática

El proceso de determinar las frecuencias de campañas de concientización para prevenir incidentes de Seguridad de la Información en la financiera se realiza en el último trimestre del año anterior, junto con la programación anual de la gerencia, para ser aplicado al año venidero,

La forma operativa empleada para esta tarea consistía en recopilar información de incidentes pasados dentro de la empresa, incidentes en el grupo retail al que pertenece la financiera, incidentes a nivel mundial más conocidos y reportes internos elaborados por el área de Seguridad de la Información. En base a esta información, se realizaba una selección de los eventos más recurrentes, y se distribuían a lo largo del año de tal manera que se completaran 24 campañas aproximadamente, recomendando qué hacer para evitar estas situaciones. Este número está calculado considerando que se envía un correo informativo cada 15 días desde el inicio del mes de marzo hasta los últimos días del mes de noviembre, y una campaña diaria durante toda la semana del 30 de noviembre, por ser el día internacional de la Seguridad de la Información.

Todo envío de correo masivo interno debía contar con la aprobación de la división de Gestión y Desarrollo Humano considerando la necesidad, el plan y las fechas de programación. La campaña era enviada por la gerencia de Seguridad de la Información, desde un correo genérico característico del área que es de conocimiento de todos los colaboradores.

Este planeamiento anual de las campañas de concientización en el área de Seguridad de la información no contaba con un método estándar para determinar la cantidad apropiada de temas a tratar que permitiera una evaluación periódica de los resultados; se basaba en una determinación empírica que complicaba la obtención de retroalimentación en cuanto a qué puntos son necesarios prevenir y reforzar en la organización.

Surge, pues, la necesidad, no solo regulatoria sino táctica, de definir una estructura que permita obtener de forma objetiva la mejor distribución de temas en las campañas

de concientización. La decisión de cuántas veces se enfatizará en la prevención de un incidente, tiene una importancia supina, ya que la aplicación de un modelo matemático nos permite la obtención de resultados confiables, objetivos, medibles, legítimos y transparentes.

El presente informe presenta la aplicación del análisis jerárquico de procesos para la selección adecuada del número de campañas de concientización. Dicha actividad solo la ejecutará la gerencia de Seguridad de la Información para los propósitos mencionados, quedando excluido cualquier otro sector de la organización.

3. Metodología

La metodología se ha estructura en base a tres grandes fases que se irán desarrollando a lo largo del capítulo, siguiendo el método del análisis jerárquico de procesos (AHP). Estas fases han sido definidas de la siguiente manera:

- Reconocimiento del problema y estructuración
- Estimaciones y evaluación
- Análisis de sensibilidad

En el Gráfico N°2 se presenta un flujo de trabajo elaborado por el autor en base a las fases indicadas en el párrafo anterior. En esta figura se detalla las actividades desarrolladas y la secuencia de estas para alcanzar el objetivo deseado.

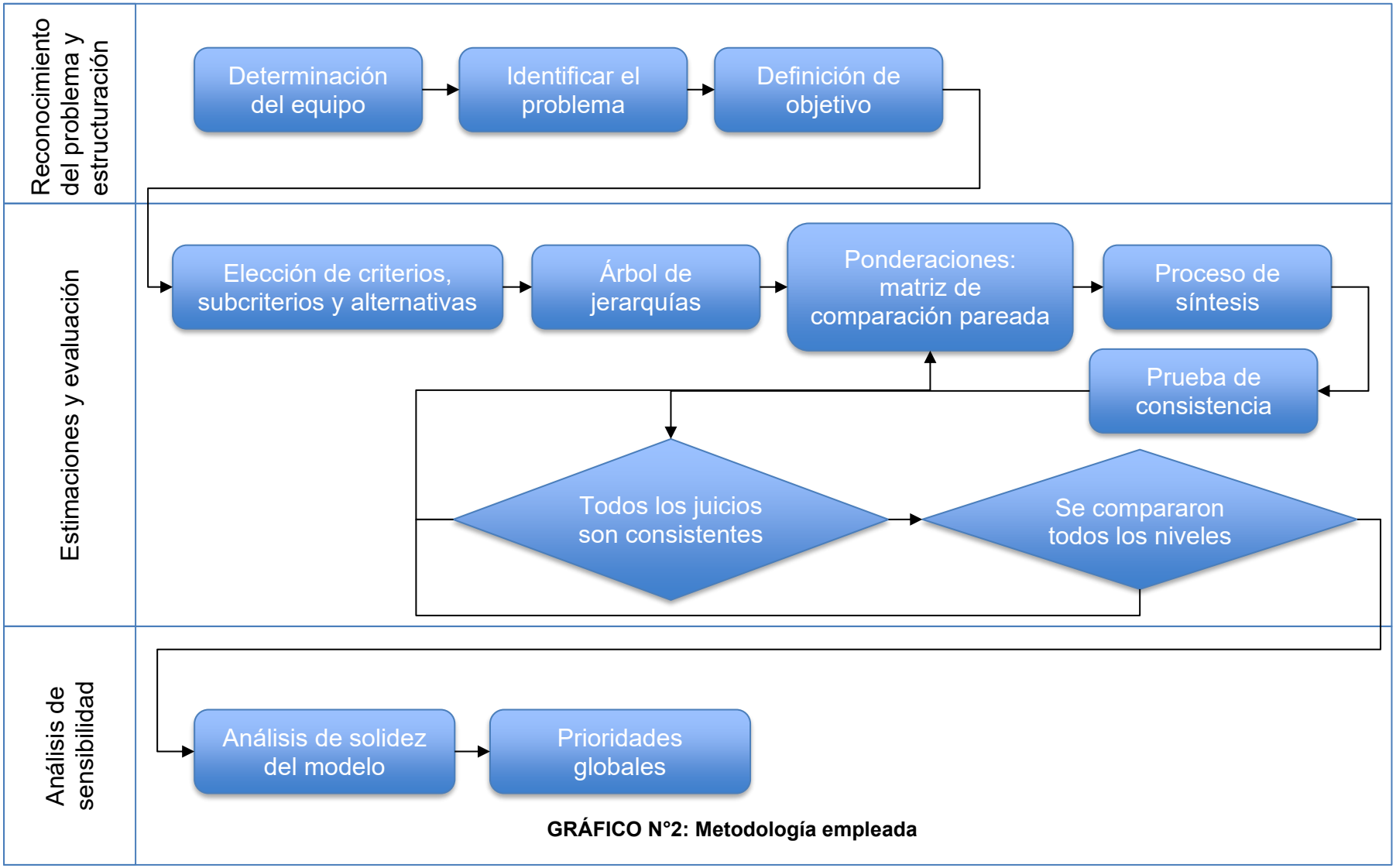

GRÁFICO N°2: Metodología empleada

3.1. Reconocimiento del problema y estructuración

3.1.1. Determinación del equipo de trabajo

La elección del equipo de trabajo fue el mismo dedicado a armar el plan anual de la gerencia, considerando para el ejercicio, además, a un especialista del área de Seguridad Informática y ciberseguridad.

El equipo está conformado por:

- Supervisor de Seguridad de la Información, experiencia de 7 años en implementación del Sistema de Gestión de Seguridad de la Información en sector retail y financiero.
- Analista de Seguridad de la Información Senior, experiencia de 5 años en la implementación del Sistema de Gestión de Seguridad de la Información y Ley de protección de datos personales.
- Analista de Seguridad de la Información Senior, experiencia de 5 años en auditoría de Seguridad de la Información y Continuidad del Negocio.
- Analista de Seguridad de la Información, encargado de la ejecución de controles de Seguridad, con 2 años de experiencia en administración de plataformas de seguridad.
- Asistente de Seguridad de la Información, encargada de la evaluación de riesgos de Seguridad.
- Analista de Seguridad Informática y Ciberseguridad, experiencia en soporte técnico y administración de herramientas de seguridad perimetral.

El gerente de Seguridad de la Información y Prevención de fraudes, que cumple el rol de Oficial de Seguridad de la Información (CISO por sus siglas en inglés: *Chief Information Security Officer*), participó como agente consultor externo y validador de la metodología.

Las sesiones se plantearon dentro de las reuniones de trabajo del área en mención, quedando documentadas en actas internas, las cuales forman actualmente parte de la documentación restringida de la organización. Para la ejecución del proyecto se indicó al equipo de trabajo el esfuerzo a realizar tanto en horas de capacitación en la herramienta como en sesiones que permitieran la discusión y sustentación de las calificaciones de cada miembro.

Adicionalmente se indicó del esfuerzo adicional por cada miembro en las consideraciones que realice para proponer o incrementar los puntos que, como guía, se brindaron para la ejecución del AHP. Entre los recursos adicionales se encuentra:

- Tiempo de recolección y análisis de información que permitiría a cada miembro, en base a fuentes y reportes tanto comunes como propias de investigación, la toma de decisiones y ponderaciones.
- Tiempo de estudio e investigación de la metodología AHP que provea de entendimiento a la hora de la aplicación del análisis.

3.1.2. Identificación del problema

Como se detalla en la sección anterior, la financiera se ha visto en la necesidad de atender los requerimientos de los entes reguladores, y uno de los puntos que se solicita es la capacitación del personal en Seguridad de la Información, de manera que los colaboradores tengan las herramientas suficientes para hacer frente a incidencias en su labor cotidiana y en su vida personal que, a raíz de la nueva normalidad, impacta en su vida laboral.

En el proceso de análisis se identificó que, al establecerse el trabajo remoto, se abandonaba el perímetro de seguridad de la organización y se reemplazaba por la red doméstica, reduciéndose la visibilidad de las actividades y aumentándose la exposición del colaborador. Se encontró, además, que el vocabulario y conocimiento de las técnicas usadas por los atacantes, no era de pleno conocimiento de los colaboradores ya que no eran términos que pertenecían a su día a día. Finalmente, es importante mencionar que en este periodo de tiempo, desde que inició la pandemia, distintos servicios y software para realizar ciberataques han sido publicados en internet y redes sociales, aumentando la probabilidad de un ciberataque.

En esta realidad, el problema que encuentra la gerencia de Seguridad de la Información es: ¿Cuántas campañas por tema, relacionado a prevenir incidentes de seguridad, deben considerarse en el plan anual?

3.1.3. Definición del objetivo

El equipo de trabajo determinó el objetivo como: “Identificar los temas y la cantidad de los mismos para las campañas de concientización que prevengan incidentes de seguridad en la organización”. Se planteó la definición del objetivo al equipo de trabajo, así como al consultor externo, de manera que evalúen la idoneidad, realicen la validación u objeción del planteamiento. La comunicación con el equipo fue de

forma remota, vía videollamada, en el cual se presentó el problema, el objetivo y la metodología a emplearse, y se indicó la forma de llenar los formatos de trabajo.

Para completar esta actividad se realizó un kick-off o presentación del proyecto, en el cual se explicó qué es el Análisis Jerárquico de Procesos, parte del marco teórico del mismo y su base matemática. Luego se presentó la metodología descrita en la Gráfico N°2 y los resultados esperados. El tiempo de duración fue de una hora.

3.2. Estimaciones y evaluación

3.2.1. Elección de criterios, subcriterios y alternativas

Criterios

La fase de estimaciones y evaluación inicia con la determinación de los criterios a utilizar en el método AHP. Para esta actividad se tomó como referencia el documento interno de Gestión de Incidentes de Seguridad de la Información elaborado por la organización que determina las fuentes de información que alimenta este proceso. Asimismo, el equipo de trabajo consideró otros criterios que fueron incluidos debido a la coyuntura del Covid-19 y los elementos regulatorios.

El Manual de Políticas para la Gestión de Incidentes de Seguridad de la Información fue entregado a cada miembro del equipo de trabajo, quienes tuvieron una ventana de tiempo de tres días para analizar el documento. Luego, fueron convocados a una sesión de dos horas en la que se les presentó el formato que utilizarían para la determinación de criterios y la forma de llenarlo.

En el documento de trabajo se les presentaba preguntas con dos opciones cerradas en base al manual de política analizado previamente; adicionalmente, se integraron preguntas abiertas, en las que los miembros del equipo, en base a su experiencia, tenían la posibilidad de adicionar puntos de vista que no fueron contemplados inicialmente.

Los criterios propuestos se basaron en los tipos de fuentes de información que incluye el documento mencionado de Gestión de incidentes, y que responden al tipo de actividad involucrada en la gestión. Además, a pedido del consultor externo, se adicionó la opción ‘Otros criterios’, los cuales debían ser justificados en la sesión y evaluados por los presentes, de manera que, dependiendo de la aceptación o no de los mismos, eran incluidos o rechazados para el proceso. En la Tabla N°1 se presenta el formato empleado por el equipo de trabajo, donde se muestra la propuesta original

de criterios. En la sección de resultados se presentarán los criterios que fueron incluidos a raíz de las reuniones y evaluaciones.

TIPOS DE FUENTES DE INFORMACIÓN	CONSIDERAR	NO CONSIDERAR
Hallazgos e incidencias		
Ejercicios de Seguridad		
Cibervigilancia		
Otros Criterios:		

TABLA N°1. Formato empleado para la identificación de criterios.

Subcriterios

La propuesta de subcriterios se basa en las fuentes de información que se mencionan en el Manual de Política para la Gestión de Incidentes de Seguridad de la Información. Sin embargo, durante la misma sesión de trabajo y de la misma forma que en la selección de criterios, se puso a consideración la adición de otros subcriterios no contemplados inicialmente. Como era de esperarse, ante el incremento de criterios, el equipo de trabajo estableció la adición de otros subcriterios los cuales derivaban de la fase anterior.

A continuación, se presenta la Tabla N°2 utilizada en el formato original. En la sección de resultados se mostrará qué otros subcriterios se añadieron a raíz de la evaluación y consenso del equipo de trabajo.

FUENTES DE INFORMACIÓN	CONSIDERAR	NO CONSIDERAR
Hallazgos e incidencias		
Registro de incidentes TI		
Amenazas del entorno		
Incidentes informados a Seguridad de la Información		
Ejercicios de Seguridad		
Ethical hacking		
Ingeniería social		
Cibervigilancia		
Amenaza del entorno		
Alertas de seguridad de externos		
Otros Subcriterios:		

TABLA N°2. Formato empleado para la identificación de subcriterios.

Alternativas

Las alternativas de decisión fueron tomadas del documento interno Gestión de Incidentes de Seguridad de la Información elaborado por la financiera, el cual recoge una clasificación estandarizada de incidentes basada en un framework internacional elaborado por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA por sus siglas en inglés: European Network and Information Security Agency). Sin embargo, se puso en consideración la adición de alguna alternativa que no haya sido contemplada inicialmente, lo cual permitió el establecimiento de otra opción en base a los criterios y subcriterios evaluados anteriormente.

Cabe destacar que algunos especialistas del rubro de Seguridad y Ciberseguridad consideran que esta clasificación no corresponde con la definición propia de un incidente de Seguridad de la Información y proponen algunos ajustes a los nombres utilizados para clasificación, sin embargo, dado que no es el objeto de este trabajo, se mantuvo la taxonomía y se optó por consenso respetar la formulación de ENISA, dado que es un referente a nivel mundial y las herramientas tecnológicas de seguridad se encuentran alineadas a este. La Tabla N°3 presenta la clasificación de los incidentes de Seguridad de la Información extraída del documento interno de la

organización, la cual no considera la alternativa adicional que será presentada en la sección de resultados.

CLASIFICACIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
Clases de Incidentes	Descripción	Ejemplo de incidente
Código malicioso	Software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red, sin el conocimiento de su responsable o usuario y con finalidades muy diversas.*	Virus.
		Gusanos.
		Troyanos.
		Spyware.
		Rootkit.
		Ransomware.
		Remote Access Tool (RAT).
Disponibilidad	Ataques dirigidos a poner fuera de servicio los sistemas, con el objetivo de causar daños en la productividad y/o imagen de las instituciones atacadas. (ENISA, 2018)	DoS / DDoS.
		Fallo (Hardware / Software).
		Error humano.
		Sabotaje.
Obtención de información	Ataques dirigidos a recabar información fundamental que permita avanzar en ataques más sofisticados, a través de ingeniería social o de identificación de vulnerabilidades. (ENISA, 2018)	Identificación de activos y vulnerabilidades (escaneo).
		Sniffing.
		Ingeniería Social.
		Phishing.
		Advanced Persistent Theat (APT).
Intrusiones	Ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, con el objetivo de introducirse de forma fraudulenta en los sistemas	Compromiso de cuenta de usuario.
		Defacement.
		Cross-Site Scripting (XSS).
		Cross-Site Request Forgery (CSRF / XSRF).
		Inyección SQL.

* Europeran for Network and Information Security Agency [ENISA], 2018.

CLASIFICACIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
Clases de Incidentes	Descripción	Ejemplo de incidente
	de una organización. (ENISA, 2018)	Spear Phishing.
		Pharming.
		Ataque de fuerza bruta.
		Remote File Inclusion (RFI).
		Explotación de vulnerabilidad software.
		Explotación de vulnerabilidad hardware.
		Acceso no autorizado a red.
Compromiso de la información	Incidentes relacionados con el acceso y fuga (confidencialidad), modificación o borrado (integridad) de información confidencial y/o restringida. (ENISA, 2018)	Acceso no autorizado a información.
		Modificación y borrado no autorizado de información.
		Publicación no autorizada de información.
		Filtración de información al exterior de la financiera.
Fraude	Incidentes relacionados con acciones fraudulentas derivadas de suplantación de identidad, en todas sus variantes. (ENISA, 2018)	Spoofing.
		Uso de recursos no autorizados.
		Uso ilegítimo de credenciales.
Contenido abusivo	Ataques dirigidos a dañar la imagen de la organización o a utilizar sus medios electrónicos para otros usos ilícitos (tales como la publicidad, la extorsión o, en general, la ciberdelincuencia). (ENISA, 2018)	Spam.
		Acoso / extorsión / mensajes ofensivos.
		Pederastia / racismo / apología de la violencia / delito, entre otros.
Política de Seguridad de la Información	Incidentes relacionados por incumplimiento de las	Abuso de privilegios por usuarios.
		Acceso a servicios no autorizados.

CLASIFICACIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
Clases de Incidentes	Descripción	Ejemplo de incidente
	políticas de seguridad aprobadas por el directorio.	Robo o préstamo de contraseñas.
		Incumplimiento de Políticas de Seguridad del Personal.
		Incumplimiento de la ley de protección de datos personales.
		Intercambio no seguro de información.

TABLA N°3: Clasificación de los Incidentes de Seguridad de la Información

En base a esta descripción, el equipo de trabajo consideró pertinente que las alternativas se identifiquen con las clases de incidentes y no con la etiqueta de la tercera columna, puesto que el tratamiento y prevención de los eventos contenidos en cada clase son los mismos.

3.2.2. Árbol de jerarquías

En base al consenso del equipo de trabajo, y a raíz de sus respuestas en cada uno de los formatos entregados, se planteó el problema a través de un árbol de jerarquías de arriba hacia abajo, el cual se organizó empezando por el objetivo, los criterios de evaluación y finalmente las alternativas.

3.2.3. Matriz de ponderaciones

Evaluación de criterios y subcriterios

Luego de haber determinado los criterios, subcriterios y alternativas, el equipo de trabajo, de forma individual, realizó una evaluación de la importancia de los criterios y subcriterios considerando el objetivo que se desea alcanzar. Los formatos fueron enviados a través de correo electrónico a los miembros del equipo de trabajo, de manera que realizaran las comparaciones usando la escala que Saaty en su libro *Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process* describe de la siguiente manera y que fue explicada a los miembros del equipo de trabajo previamente.

Intensidad de importancia	Definición	Explicación
1	Igual importancia	Dos actividades contribuyen igualmente al objetivo.
2	Débil o ligeramente	
3	Moderada importancia	La experiencia y el juicio favorecen ligeramente a una actividad sobre la otra.
4	Más moderada	
5	Mayor importancia	La experiencia y el juicio favorecen fuertemente a una actividad sobre la otra.
6	Más fuerte	
7	Muy fuerte o demostrada importancia	Una actividad es favorecida muy fuertemente sobre la otra, su dominio demostrado en la práctica.
8	Muy, muy fuerte	
9	Extrema importancia	La evidencia favorece una actividad sobre la otra, es el orden de afirmación más alto posible.

TABLA N°4: La escala fundamental de números absolutos[†]. (Saaty, 2013)

Para efectos de la evaluación, se envió un modelo el cual se detalla en el Gráfico N°3 y Gráfico N°4, donde se muestra el objetivo validado por el equipo, los criterios y subcriterios identificados.

[†] The fundamental scale of absolute numbers (Saaty, 2013).



GRÁFICO N°3. Ejemplo de comparación de criterios

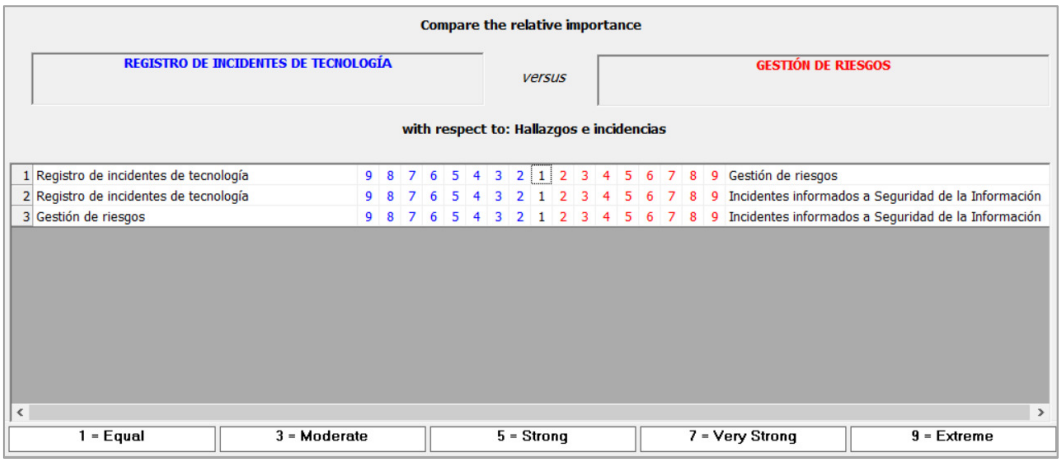

GRÁFICO N°4. Ejemplo de comparación de subcriterios

Esta información se recopiló en formatos Excel preparados para realizar el análisis y estimar resultados preliminares. Fueron enviados a cada miembro del equipo de trabajo para el llenado respectivo.

Evaluación de alternativas

Ante la existencia de gran cantidad de tipos de incidentes de Seguridad de la Información, los cuales van aumentando y diversificándose, usando un mismo vector de ataque, lo que permite dar un mismo tratamiento por tipo de incidente, el equipo de trabajo decidió tomar la clasificación de incidentes como las alternativas, agrupando los incidentes de acuerdo con la clasificación realizada por ENISA. Para la comparación se utilizará la escala descrita en la Tabla N°4 del apartado anterior.

Las respuestas del equipo de trabajo fueron registradas en documentos Excel individuales proporcionados a cada uno. Estos archivos digitales fueron preparados

por el Supervisor de Seguridad de la Información, considerando los elementos adicionales que resultaron del debate en las sesiones de trabajo. La finalidad de estos documentos era registrar las evaluaciones de cada miembro, de tal manera que, en base a la evaluación por criterios y subcriterios de las alternativas consensuadas, cada uno tenga un resultado de la priorización de los incidentes de Seguridad de la Información a los que se dedicará, por nivel de importancia y de acuerdo al criterio del evaluador, un número determinado de campañas de concientización a lo largo del año.

Proceso de síntesis

El equipo de trabajo tuvo diez días calendario para emitir sus ponderaciones y remitir el formato Excel debidamente llenado. Al recopilar toda la información, el Supervisor de Seguridad de la Información se encargó de sintetizar todos los archivos en el programa Expert Choice, el cual permitió visualizar las comparaciones hechas por cada miembro del equipo de trabajo y las alternativas priorizadas, así como el análisis conjunto de las evaluaciones.

Prueba de Consistencia

La consistencia de una matriz de comparación está determinada por la razón de consistencia, evaluada para cada criterio que se ha determinado usar en el análisis jerárquico.
Esta razón debe ser de 10%, y Saaty nos explica que el requisito porcentual no puede reducirse, como al 1% o al 0.1%, sin trivializar el impacto de la incoherencia. La inconsistencia misma es importante, puesto que sin ella, no se puede admitir el nuevo conocimiento que cambia de preferencia. Asumir que todo el conocimiento debe ser consistente contradice la experiencia que requiere un ajuste continuo en la comprensión. De hecho, en el ámbito de la tecnología, este rango de inconsistencia aceptada permite esa flexibilidad propia de la realidad que va en constante cambio y evolución. Por lo tanto, el objetivo de desarrollar un marco coherente de amplio alcance depende de admitir alguna incoherencia.

Sin embargo, no siempre esta razón es del 10%, Saaty especifica que por convención, la razón de consistencia debe ser de 5% y 8% para n=3 y 4 respectivamente, donde “n” refiere a la cantidad de opciones con las que estamos trabajando el AHP. Para todos los valores de n≥5 la razón de consistencia es de 10%[‡] (Saaty, 2013). Es en

[‡] “By noting the Random Inconsistency Indices for different values of n, we distribute 10% proportionally by multiplying it by each of the R.I. values. These percentages are suggested by the R.I. values above. In other words, if the R.I. is equal to 1 for all n, we would allow 10% in all cases. However, for n = 3 and 4, the values are 0.52 and 0.89 and for n ≥ 5 it is greater than one. By convention we require the consistency ratio to be 5% and 8% for n = 3 and 4 respectively and 10% for all values of n ≥ 5. A

esta línea que el equipo de trabajo, de acuerdo a la cantidad de alternativas con las que contaba, trabajó con la razón de consistencia de menor o igual a 10%.

Uno de los datos que son necesarios para encontrar la razón de consistencia es el índice de consistencia aleatorio (IA) para las diferentes cantidades de opciones que se tengan, cada uno de los cuales es un índice promedio calculado por E. Forman.

n=	1	2	3	4	5	6	7	8	9	10
I.A.	0	0	.52	.89	1.11	1.25	1.35	1.40	1.45	1.49

n=	11	12	13	14	15
I.A.	1.51	1.54	1.56	1.57	1.58

TABLA 5. Índices de consistencia Aleatorios (IA). Fuente: Saaty, 2013.

El otro factor indispensable para calcular la razón de consistencia (RC) está determinado por el índice de consistencia de la matriz (IC), el cual se calcula en una operación matemática donde interviene la cantidad de alternativas, y el λ_{max}, que resulta de la multiplicación de la matriz normalizada y la matriz original.

Cabe destacar que todo este proceso ha sido realizado en el documento Excel entregado a cada miembro y, obviamente, en el software Expert Choice que sintetiza todos los formularios llenados por el equipo de trabajo, así como la evaluación de la consistencia.

3.3. Análisis de sensibilidad

3.3.1. Análisis de solidez del modelo

Antes de definir los resultados finales, se eligieron los criterios con mayor grado de inconsistencia, es decir, los más cercanos al RC=10%, y se asignaron valores aleatorios a los criterios asociados para analizar si las alternativas mantenían su consistencia o se alcanzaba alguna variación significativa en las prioridades.

3.3.2. Prioridades globales

plausible approach to the measurement of inconsistency has also been given by Golden and Wang." (Saaty, 2013).

Finalmente, luego de que el equipo de trabajo realizó las ponderaciones, se emitió juicios, se midió la consistencia y evaluó la sensibilidad del modelo, se obtuvo el resultado final basado en la decisión de los expertos y puesto a validación del consultor externo.

Cabe señalar que en la presentación de los resultados, el consultor externo eligió al azar comparaciones para sustentar el motivo de las calificaciones, así tenía la certeza que las ponderaciones fueron determinadas con un criterio razonable.

3.4. Resultados

3.4.1. Reconocimiento del problema y estructuración

Definición de objetivo

El objetivo fue definido de la siguiente manera: Identificar los temas y la cantidad de los mismos para las campañas de concientización que prevengan incidentes de seguridad en la organización. Esta definición fue validada por el equipo de trabajo y el consultor externo como el adecuado para el modelo definido.

Identificación de criterios, subcriterios y alternativas

El equipo de trabajo, en base a las opciones que se les presentó en los formatos, validaron los siguientes criterios:

- **Hallazgos e incidencias**: Se consideran todos los incidentes de seguridad en la organización, entorno financiero, grupo económico y nivel nacional.
- **Ejercicios de Seguridad:** Se considera los resultados de los ejercicios de Seguridad y Ciberseguridad ejecutados en la empresa.
- **Cibervigilancia:** Se consideran todos los incidentes a nivel latinoamérica y mundial, así como reportes de las empresas tecnológicas por vulnerabilidades encontradas.
- **Regulaciones:** Este criterio fue propuesto y agregado por los miembros del equipo de trabajo. Se consideran los puntos exigidos por los entes reguladores.
- **COVID-19**: Este criterio, al igual que el anterior, fue propuesto y agregado por el equipo de trabajo. Se tomó en cuenta debido a las consideraciones adicionales que se debe seguir para proteger la información a raíz de la nueva normalidad.

En base a los criterios validados por el equipo de trabajo se presentó las opciones de subcriterios donde se planteó:

- Hallazgos e incidencias
    - Registro de incidentes de tecnología: Esta elección se basó en los reportes de perfomance de la organización y el registro de incidencias de tecnología que la empresa mantiene.
    - Gestión de riesgos: Como parte del Sistema de Gestión de Seguridad de la Información, la gestión de riesgos permite conocer los activos de información que participan en los procesos de la organización, así como los riesgos asociados a los mismos.
    - Incidentes informados a Seguridad de la Información: Se basa en el registro de incidentes de Seguridad de la Información de la organización, el cual tiene como fuente principal los reportes de los colaboradores.
- Ejercicios de Seguridad
    - Ethical Hacking: las pruebas de intrusión realizadas a la organización permiten detectar puntos de mejora en la seguridad. Es por ello que los resultados e informes de estas pruebas fueron considerados como subcriterios para determinar la priorización de las alternativas.
    - Ingeniería Social: este ejercicio se realiza de manera recurrente en la organización, lo que permite tener un subcriterio relacionado a la cantidad de personas que participaron de las pruebas y no tuvieron un accionar esperado.
- Cibervigilancia
    - Alertas de Seguridad de externos: la organización contrata un servicio dedicado a informar a la empresa sobre vulnerabilidades encontradas en servicios tecnológicos, nuevas variantes de malware y/o ransomware y campañas de hacktivismo.
    - Amenazas del entorno: el corporativo al que pertenece Financiera Oh comparte con las empresas miembros del grupo retail cualquier tipo de caso que pueda afectar la seguridad de cada organización.
- Regulaciones
    - Ley de protección de datos personales: La ley 27933 regula a todas las organizaciones y establece directivas de seguridad organizacional, técnicas y legales que deben ejecutar las empresas peruanas para proteger los datos personales que almacenan y transmiten. Una de estas directivas tiene relación directa con la gestión de incidentes que puedan afectar banco de datos personales, así como la concientización del personal en esta materia.

    - Reglamento SBS 504-2021: El ente regulador financiero publicó este reglamento en el cual indica las medidas de seguridad a considerar para una correcta aplicación del Sistema de Gestión de Seguridad de la Información y Ciberseguridad. Está basado en estándares internacionales como ISO/IEC 27001:2013, ISO/IEC 27032 y NIST.
- COVID-19:
    - Home office: La nueva normalidad cambió los esquemas de trabajo, de modo que el colaborador, que en la organización tenía todas las medidas de seguridad tecnológica para prevenir incidentes, desde su hogar no las tenía; en este contexto está más expuesto a ataques, suplantaciones y fraudes.
    - Ciberterrorismo: Uno de los delitos que se han presentado con mayor frecuencia desde que comenzó la pandemia fue el ciberterrorismo. Una serie de ataques a entidades, negocios, micro-empresarios y grandes corporaciones con el fin de obtener dinero o reputación en la dark-web.

Finalmente se eligieron las siguientes alternativas en base al documento de la organización de Gestión de Incidentes de Seguridad de la Información luego del análisis de los criterios y subcriterios ya definidos:

- Código malicioso
- Disponibilidad
- Obtención de información
- Intrusiones
- Compromiso de la información
- Fraude
- Contenido abusivo
- Política de Seguridad de la Información
- Ciberseguridad en casa

El equipo de trabajo decidió agregar la alternativa de ‘ciberseguridad en casa’ a raíz de la nueva normalidad por el COVID-19, quedando finalmente nueve alternativas de decisión para la aplicación del Análisis Jerárquico de Procesos.

Árbol de jerarquías

En base a las respuestas de todo el equipo de trabajo, se estructuró el árbol jerárquico. Se planteó con tres niveles de orden, los cuales son: objetivo, criterios, subcriterios y alternativas. Estos pueden verse en la siguiente figura elaborada por el autor, Gráfico N°5.

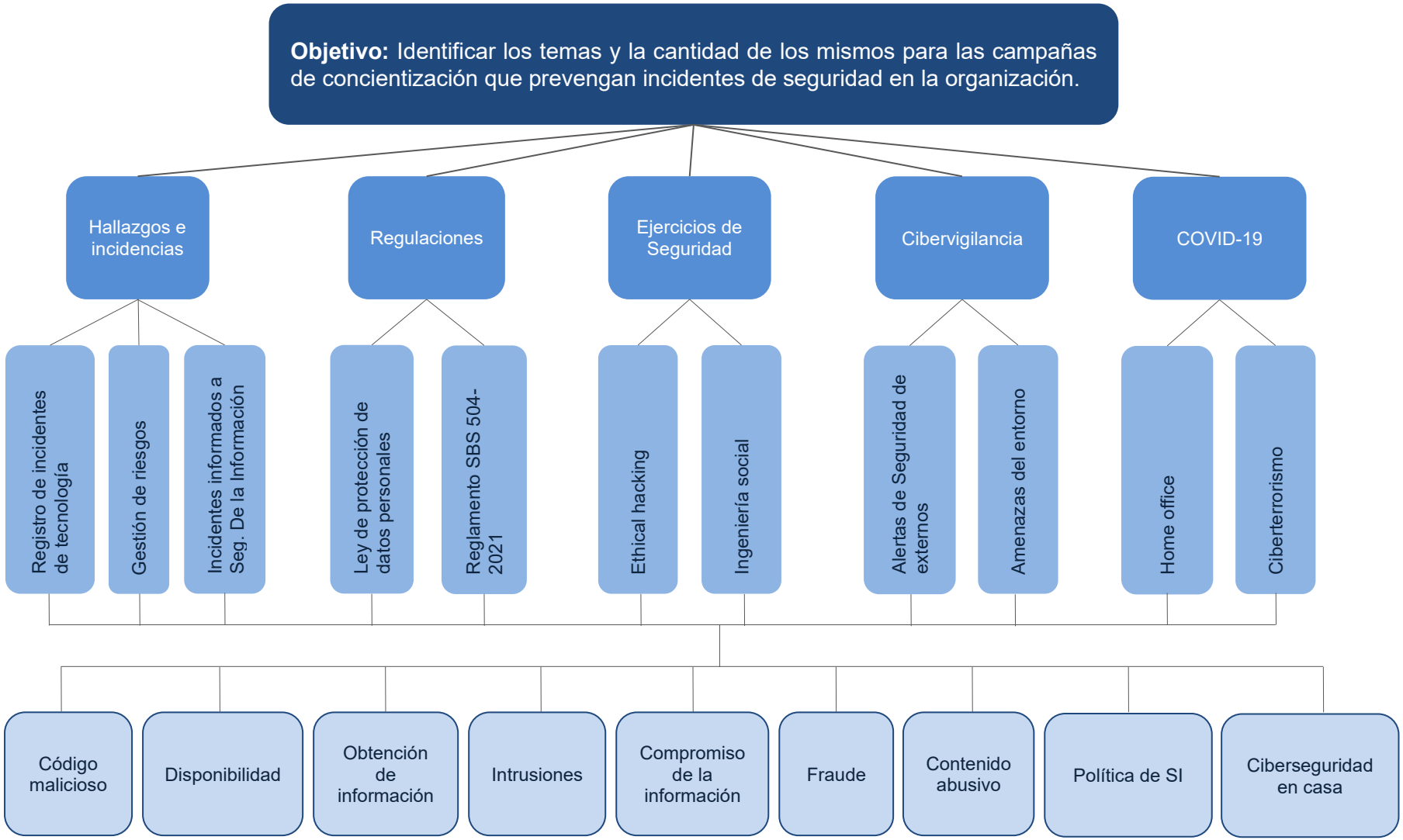

GRÁFICO N°5: Árbol de Jerarquías

3.4.2. Estimaciones y evaluación

El equipo de trabajo emitió sus valoraciones al comparar las alternativas en base a cada subcriterio y criterio definido. Los resultados fueron ingresados en el software Expert Choice, respetando la valoración de cada miembro, para luego ejecutar la combinación de los resultados de los participantes. En total fueron seis valoraciones independientes que mantuvieron una razón de consistencia de las alternativas respecto al objetivo de 0.01, lo cual indica que es consistente el resultado.

En base a la información ingresada y procesada, se obtuvo que el criterio con mayor valoración fue Hallazgos e incidencias con 27.3%, seguido por Ejercicios de Seguridad con 24.1% y Regulaciones con 22.4%. Los dos criterios que obtuvieron un porcentaje menor marcan una distancia considerable respecto al resto: Covid-19 obtuvo 13.5% y Cibervigilancia 12.7%. En el Gráfico N°6, podemos visualizar los resultados gráficos del software y la inconsistencia de los criterios respecto del objetivo es de 0.02:

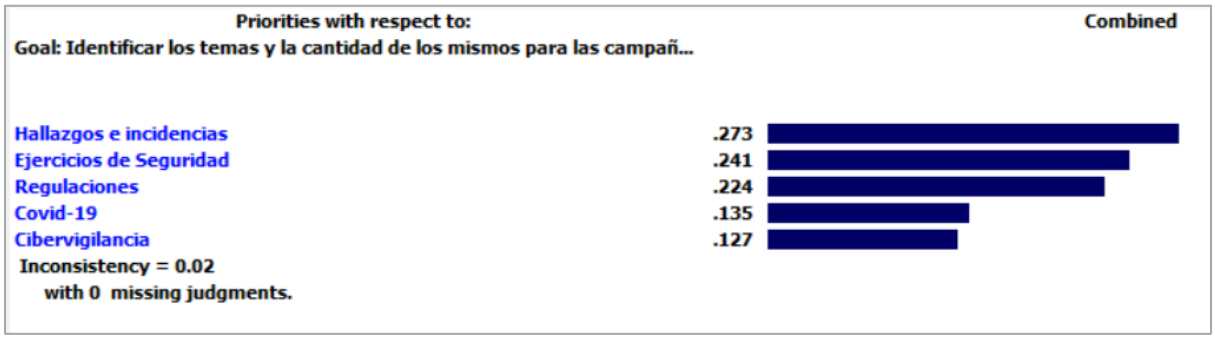

GRÁFICO N°6: Criterios con respecto al objetivo

Al efectuar la síntesis de los subcriterios con respecto del objetivo, podemos identificar la importancia relativa de los subcriterios. El criterio Ejercicios de seguridad subcriterio Ingeniería Social ha resultado con mayor importancia para el objetivo de identificar los temas y la cantidad de los mismos para las campañas de concientización que prevenga incidentes de Seguridad de la Información con un 15.4%, le sigue Ethical hacking con 8.7%; en relación al criterio Regulaciones subcriterio Reglamento SBS-504-2021 alcanzó un porcentaje de 12.6%, mientras que Ley de Protección de Datos Personales alcanzó 9.8%. En el criterio Hallazgos e incidencias subcriterio Incidentes informados a seguridad de la Información, el porcentaje fue de 11.7%, Registro de incidencias de TI, 9.1% y Gestión de riesgos, 6.5%. Los subcriterios subordinados a Cibervigilancia y Covid-19 obtuvieron porcentajes menores, siendo en su mayoría menores a ocho puntos porcentuales. Alertas de seguridad externos obtuvo 5.6% mientras que Amenazas del entorno no superó los 7.1%. Ante la nueva normalidad

se esperaba que Home office obtuviera un puntaje mayor, sin embargo los resultados arrojan un 8.3% de importancia para el subcriterio perteneciente a Covid-19 y el puntaje más bajo para ciberterrorismo, con 5.2%. Este último se puede explicar por el aún incipiente desarrollo tecnológico que mayormente se concentra en la capital peruana, siendo poco llamativo para los delincuentes cibernéticos internacionales.

Finalmente se realizó la síntesis con respecto del objetivo planteado por el equipo de trabajo, obteniéndose la relevancia de las alternativas con respecto a este. El Gráfico N°7 muestra los resultados y los puntos porcentuales asociados a los mismos.

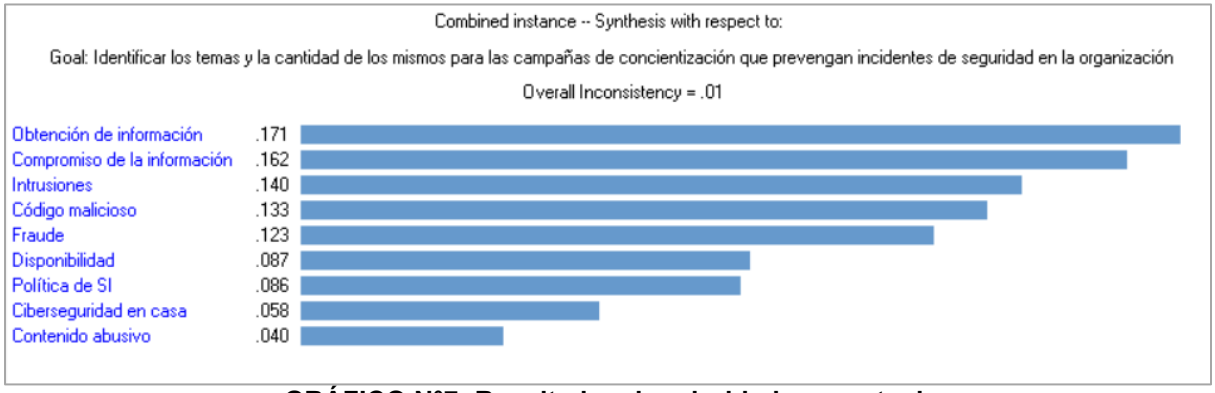

GRÁFICO N°7: Resultados de prioridad porcentual

Estos resultados podemos sintetizarlos en el árbol de jerarquías, de modo que podamos identificar la relevancia de los criterios, subcriterios y alternativas con respecto al planteamiento del equipo de trabajo en su objetivo.

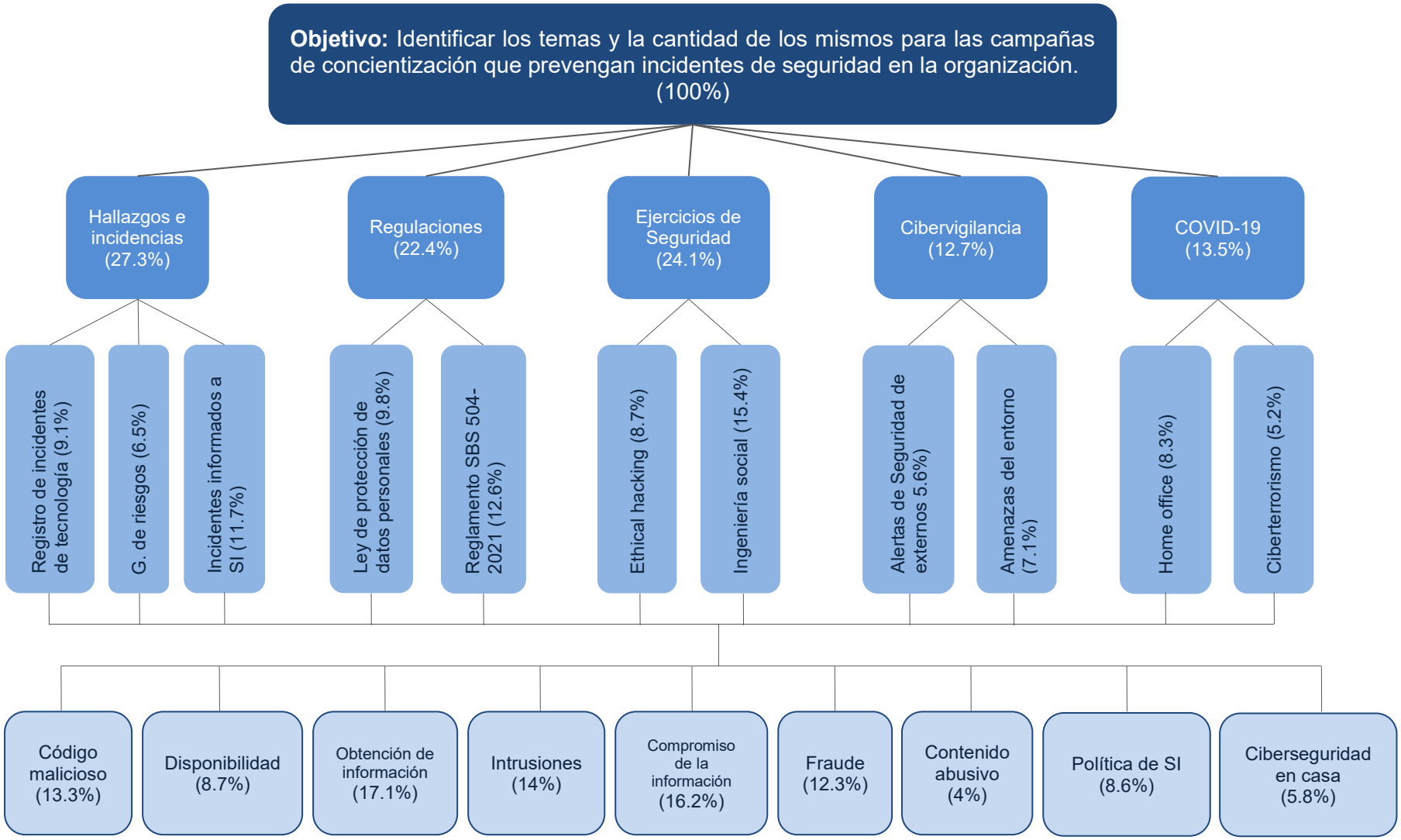

GRÁFICO N°8: Prioridad de criterios, subcriterios y alternativas de acuerdo con el objetivo

Considerando la cantidad de días durante el año asignados a Seguridad de la Información para realizar sus campañas de concientización relacionadas a las alternativas resultantes, en total veinticuatro días, se procede a calcular la cantidad de comunicaciones mediante ponderaciones, quedando la distribución como se muestra en la Tabla N°6:

ALTERNATIVA	PORCENTAJE PRIORIDAD
Obtención de información	4
Compromiso de la información	4
Intrusiones	4
Código malicioso	3
Fraude	3
Disponibilidad	2
Política de Seguridad de la Información	2
Ciberseguridad en casa	1
Contenido abusivo	1

TABLA N°6: Resultados de campañas a enviar por tipo de incidente

Análisis de sensibilidad

A pesar de haber conseguido índices de consistencia muy por debajo de lo permitido, en base a los resultados, se decidió modificar los valores obtenidos para los criterios. En la siguiente gráfica se muestran los resultados del AHP sin modificación:

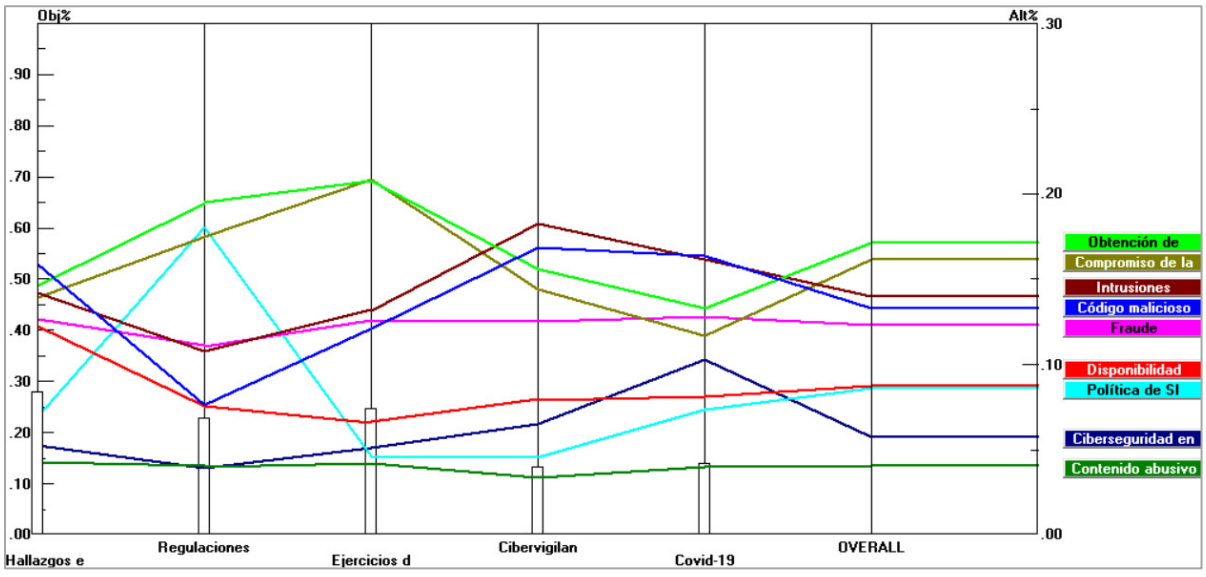

GRÁFICO N°9: Performance del análisis de sensibilidad

Se procedió a asignar 20% a los criterios para analizar el comportamiento de las alternativas, obteniéndose los resultados mostrados en el Gráfico N°10:

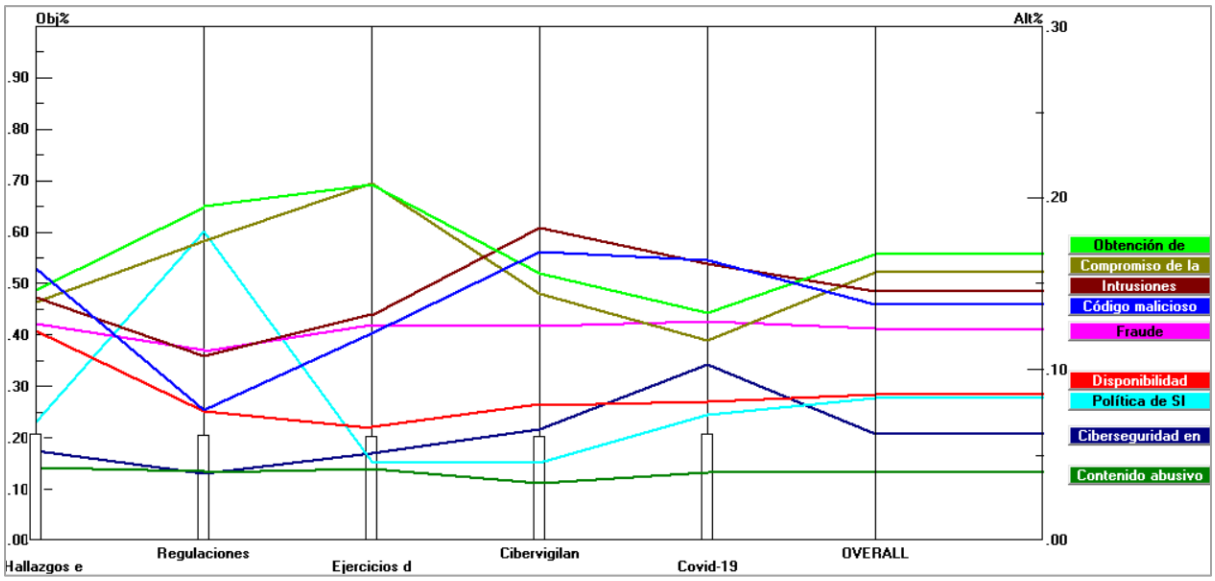

GRÁFICO N°10: Performance del Análisis de Sensibilidad. Criterios al 20%

Se puede evidenciar que la priorización de las alternativas no se ha visto afectadas en este escenario, manteniéndose la distribución original y marcándose la diferencia en tres secciones.

Continuando con el análisis, procederemos a asignar a COVID-19 un 60% y al resto 10%, con el objetivo de ver cuánto logra cambiar la decisión.

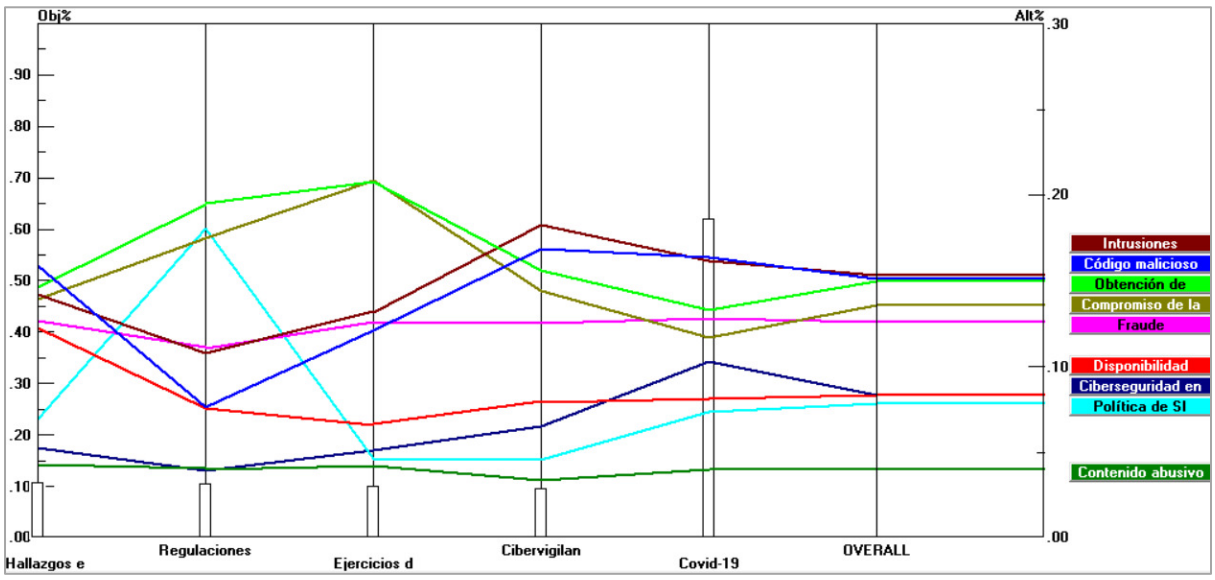

GRÁFICO N°11: Performance del Análisis de Sensibilidad. Covid-19 al 60%

A pesar de que el orden de las prioridades ha variado de acuerdo a lo que muestra el Gráfico N°11, se sigue manteniendo segmentado los grupos en tres secciones que determinarán la cantidad de campañas, las cuales se ven mínimamente afectados en la asignación.

Finalmente, se asigna a COVID-19 y Cibervigilancia un 35% y al resto 10% para ver el comportamiento de las priorizaciones, sin embargo el escenario es muy parecido al anterior y haciendo la respectiva ponderación, los cambios en la asignación de cantidades de campañas es mínimo, como se muestra en el Gráfico N°12.

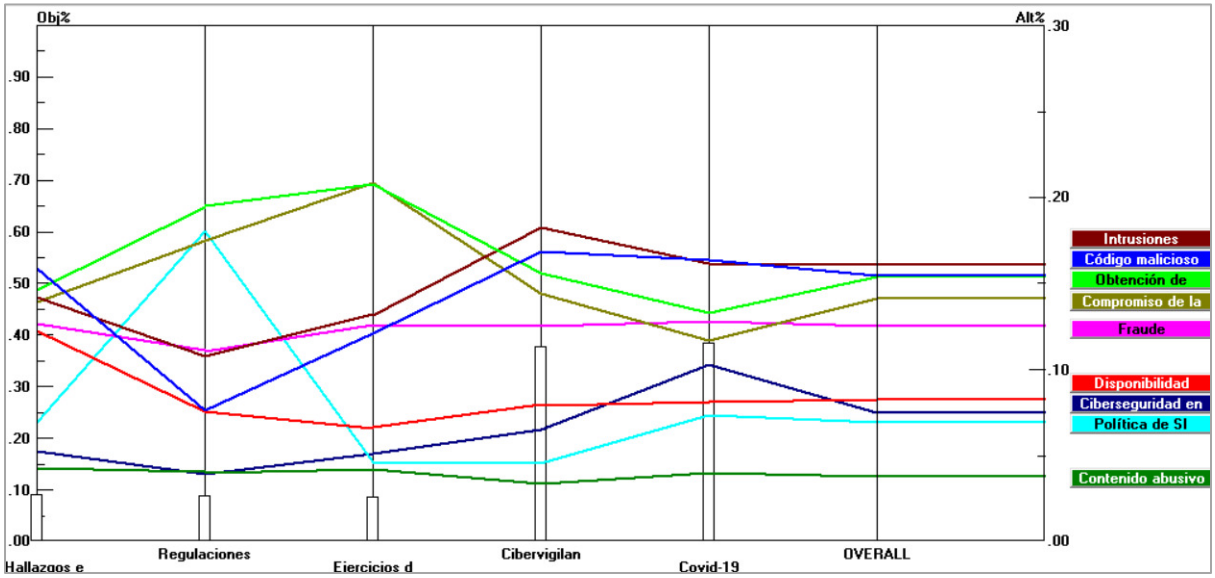

GRÁFICO N°12: Performance de Análisis de Sensibilidad. Covid-19 y Cibervigilancia a 35%

IV. CONCLUSIONES

En base a lo analizado con la herramienta AHP, se pueden llegar a distintas conclusiones y recomendaciones para aplicar en la empresa, de tal modo que se optimice el tiempo, reduciendo la cantidad de horas que se dedica a la planificación y obteniendo mayor beneficio en cuanto a carga laboral.

- Los tipos de incidentes que conllevan información han sido considerados como uno de los puntos más importantes a reforzar. El contexto propio de pandemia y actualmente la forma híbrida de trabajar, conlleva a que la seguridad se derive al colaborador y su infraestructura de red en casa; por tanto, se debe evaluar mecanismos o nuevas tecnologías que permitan asegurar los equipos y las conexiones, de modo que la seguridad no dependa tan solo del colaborador, sino que tenga un aliado en la tecnología.
- Se debe considerar y evaluar que las campañas para evitar incidentes de Seguridad de la Información con calificación o ponderación baja, pueden suprimirse en los próximos años para enfatizar en aquellos casos más recurrentes y graves. Es importante considerar, además, la madurez y el nivel de rotación de los colaboradores, ya que ello determinará una aproximación más cercana a la realidad organizacional.
- Se debe considerar los incidentes ambientales como ransomware o phishing personalizado, que han sido críticos durante el año de pandemia en las empresas del rubro financiero, al verse expuestos los colaboradores a un ambiente de trabajo distinto al que ya estaban acostumbrados con todas las medidas de seguridad.
- Evaluar la posibilidad de incrementar los criterios, a partir del recojo de información de otras áreas que influyan directamente en la cadena del negocio.

V. RECOMENDACIONES

Dado el entorno cambiante y el constante incremento de modalidades para materializar incidentes de seguridad, no basta una concientización reactiva, es decir, como respuesta a los sucesos en los entornos especificados en la aplicación de la metodología AHP, sino una concientización que, en la medida de lo posible, se adelante a los sucesos.

Si bien es cierto, esta planificación se realiza a inicios de año y en base a información tomada de fuentes internas y externas, debemos tomar en cuenta que no es estática y se necesita sumar interacciones. En ese sentido, generaría un valor adicional la medición en tiempo real, o por periodos, de los mismos criterios considerados en el análisis jerárquico de procesos aplicado. Así las campañas responderían a un escenario más actual en caso se tengan situaciones como el COVID 19 que incrementaron los ataques cibernéticos.

Se ve necesario la consideración del perfil del colaborador para medir su evolución en cuanto a la concientización, lo cual podría sumar un criterio adicional al análisis realizado y posiblemente nuevas alternativas. No obstante, esto implica la implementación de una herramienta que realice ejercicios de seguridad reales y controlados, así como el registro del comportamiento de cada uno de los colaboradores para obtener datos que permitan medir lo indicado al inicio de este párrafo.

Finalmente debemos considerar que estos esfuerzos reducen los riesgos a los que están expuestos los colaboradores, mas no lo eliminan. El entrenamiento y nuevas formas de concientización ayudarán a que estos temas sean interiorizados y la herramienta AHP es un aliado estratégico en ello.

REFERENCIAS

Fortinet (24 de febrero de 2021). *América Latina sufrió más de 41 billones de intentos de ciberataques en 2020.* https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2021/latin-america-suffered-more-than-41-billion-cyberattack-attempts-in-2020

Financiera Oh! S.A. (Noviembre de 2021). *Nuestra historia.* Recuperado el 20 de noviembre de 2021, de https://tarjetaoh.pe/quienes-somos#historia

Financiera Oh! S.A. (Noviembre de 2021). *Organigrama general.* Recuperado el 20 de noviembre de 2021, de https://static.tarjetaoh.pe/wp-content/uploads/2021/11/Organigrama_General.pptx

Superintendencia de Banca, Seguros y AFP (02 abril de 2009). *Circular N° G-140-2009.* https://intranet2.sbs.gob.pe/dv_int_cn/249/v1.0/Adjuntos/g-140-2009.c.doc

Superintendencia de Banca, Seguros y AFP (19 de febrero de 2021). *Resolución S.B.S. Nº 504-2021.* https://intranet2.sbs.gob.pe/dv_int_cn/2046/v2.0/Adjuntos/504-2021.R.pdf

Superintendencia de Banca, Seguros y AFP (02 abril de 2009). *Circular N° G-140-2009.* https://www.sbs.gob.pe/Portals/0/jer/Auto_Nuevas_Empresas/Normas_Comunes/9.%20Gesti%C3%B3n%20de%20la%20Seguridad%20de%20la%20Informaci%C3%B3n_Circ.%20SBS%20G-140-2009.pdf

Congreso de la República (02 de julio de 2011). Lima, Perú. *Ley de Protección de Datos Personales N° 29733* Recuperado el 25 de junio de 2022, de http://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

Ministerio de Justicia y Derechos Humanos (04 de mayo de 2017). *Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales.* https://www.minjus.gob.pe/wp-content/uploads/2013/11/Directiva-de-Seguridad-DGPDP.pdf

International Organization for Standardization & International Electrotechnical Commission - ISO & IEC. (15 de octubre de 2005). *Tecnología de la Información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requerimientos.* ISO/IEC 27001, Primera edición.

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI (30 de mayo de 2007). *NTP-ISO/IEC 17799:2007: Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información.* https://webs.um.es/einiesta/miwiki/lib/exe/fetch.php%3Fid%3Ddocencia%26cache%3Dcache%26media%3Disoiec17799.pdf

Europeran for Network and Information Security Agency – ENISA. (26 de abril de 2018). *Reference Incident Classification Taxonomy*. https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

Toskano, G. (2005). *El Proceso de análisis jerárquico (AHP) como herramienta para la toma de decisiones en la selección de proveedores : aplicación en la selección del proveedor para la Empresa Gráfica Comercial MyE S.R.L.* Universidad Nacional Mayor de San Marcos. Facultad de Ciencias Matemáticas. EAP. Investigación Operativa. http://sisbib.unmsm.edu.pe/bibvirtualdata/Tesis/Basic/toskano_hg/toskano_hg.pdf

Alvarez, M., Arquero, A. & Martínez, E. (2014). *Empleo Del AHP (Proceso Analítico Jerárquico) Incorporado En SIG para definir el emplazamiento óptimo de equipamientos universitarios. Aplicación a una biblioteca.* Facultad de Informática (U.P.M.) Campus de Montegancedo, 28660 Boadilla del Monte (Madrid). http://www.pronacose.gob.mx/pronacose14/Contenido/Documentos/EMPLEO_AHP_ARTICULO.pdf

Arancibia, S., Contreras, E. , Mella, S. , Torres P. & Villablanca, I. (2003). *Evaluación Multicriterio: aplicación para la formulación de proyectos de infraestructura deportiva*. Universidad de Chile. Facultad de Ciencias Físicas y Matemáticas. Ingeniería Industrial. Centro de Gestión (CEGES). http://www.dii.uchile.cl/~ceges/publicaciones/ceges48.pdf

Maurtua, D. (2006). Capítulo II: La toma de decisiones. En *Criterios de selección de personal mediante el uso del proceso de análisis jerárquico : aplicación en la selección de personal para la Empresa Exotic Foods S.A.C.* Universidad Nacional Mayor de San Marcos. Facultad de Ciencias Matemáticas. EAP. Investigación Operativa. http://sisbib.unmsm.edu.pe/bibvirtualdata/monografias/basic/maurtua_od/cap2.pdf

International Organization for Standardization & International Electrotechnical Commission - ISO & IEC. (01 de mayo de 2009). *Information technology - Security techniques - Information security management systems - Overview and vocabulary.* ISO/IEC 27000, First edition.

Saaty, T. (2013). *Theory and Applications of the Analytic Network Process: Decision Making with Benefits, Opportunities, Costs, and Risks.* USA: RWS Publications.

Anderson, D. (2004). *Métodos cuantitativos para los negocios*. México: Cengage Learning Editores S.A.

Saaty, T. (2013). *Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process.* USA: RWS Publications.

Forman, E.H. (1990). *Random Indices For Incomplete Pairwise Comparison Matrices*. European Journal of Operational Research 48, 153-155.